NPS-AS-93-020

NAVAL POSTGRADUATE SCHOOL

Monterey, California

Industrial Security Costs:
An Analysis of
Reporting Practices

Joseph G. San Miguel

August 31, 1993

Prepared for: Resources Working Group
National Industrial Security Program
Washington, D. C.

NAVAL POSTGRADUATE SCHOOL
Monterey, California

RADM T. A. Mercer
Superintendent

Harrison Shull
Provost

This report was prepared and funded by The Resources Working Group, National Industrial Security Program, Washington, D. C.

This report was prepared by:

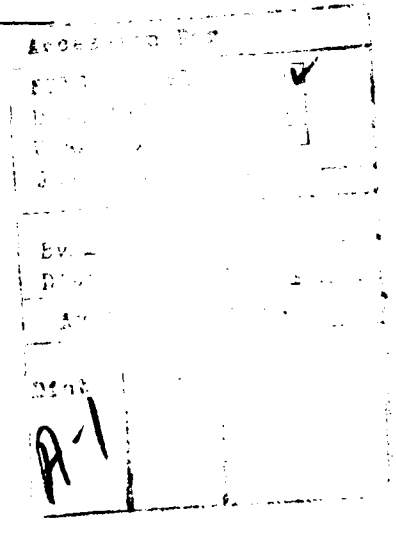
Joseph G. San Miguel
Professor
Department of Administrative Sciences

Reviewed by:

David R. Whipple, Chairman
Department of Administrative Sciences

Released by:

Paul J. Mario
Dean of Research



UNCLASSIFIED
SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION / AVAILABILITY OF REPORT Approved for public release; distribution is unlimited
2b. DECLASSIFICATION / DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) NPS-AS-93-020	5. MONITORING ORGANIZATION REPORT NUMBER(S) NPS-AS-93-020
6a. NAME OF PERFORMING ORGANIZATION NAVAL POSTGRADUATE SCHOOL 6b. OFFICE SYMBOL (If applicable) AS	7a. NAME OF MONITORING ORGANIZATION NAVAL POSTGRADUATE SCHOOL
6c. ADDRESS (City, State, and ZIP Code) Administrative Sciences Department Naval Postgraduate School Monterey, CA 93943-5000	7b. ADDRESS (City, State, and ZIP Code) Superintendent Naval Postgraduate School Monterey, CA 93943-5000
8a. NAME OF FUNDING / SPONSORING ORGANIZATION Resources Working Group 8b. OFFICE SYMBOL (If applicable)	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER PERSEREC
8c. ADDRESS (City, State, and ZIP Code) Resources Working Group National Industrial Security Program	10 SOURCE OF FUNDING NUMBERS PROGRAM ELEMENT NO / PROJECT NO / TASK NO / WORK UNIT ACCESSION NO
11. TITLE (Include Security Classification) Industrial Security Costs: An Analysis of Reporting Practices UNCLASSIFIED	
12. PERSONAL AUTHOR(S) Joseph G. San Miguel	
13a. TYPE OF REPORT Technical 13b TIME COVERED FROM _____ TO _____	14. DATE OF REPORT (Year, Month, Day) August 1993 15 PAGE COUNT 35
16 SUPPLEMENTARY NOTATION	
17 COSATI CODES FIELD / GROUP / SUB-GROUP	18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)

19 ABSTRACT (Continue on reverse if necessary and identify by block number)

This report summarizes a research study of the accounting for and reporting of industrial security costs. Eight organizations participated in the field research which was sponsored by the Resources Working Group of the National Industrial Security Program. The research sites span classified and special security programs for the Department of Defense, the Central Intelligence Agency, and the Department of Energy. The objective was to evaluate whether or not cost information could be gathered by a questionnaire on a periodic basis. The research findings include a wide diversity of security cost practices, a lack of uniformity in cost allocations, and differing organization structures for security operations. Several recommendations are made to support an initial cost gathering methodology.

20. DISTRIBUTION / AVAILABILITY OF ABSTRACT ☒ UNCLASSIFIED/UNLIMITED ☐ SAME AS RPT ☐ DTIC USERS	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL Joseph G. San Miguel	22b. TELEPHONE (Include Area Code) (408) 656-2187 22c. OFFICE SYMBOL

INDUSTRIAL SECURITY COSTS: AN ANALYSIS OF REPORTING PRACTICES

By

Joseph G. San Miguel, Ph.D., CPA
Professor of Financial Management
Naval Postgraduate School
Monterey, California 93943

Prepared
For

Resources Working Group
National Industrial Security Program
Washington, DC

August 31, 1993

INDUSTRIAL SECURITY COSTS: AN ANALYSIS OF REPORTING PRACTICES

Abstract

This report summarizes a research study of the accounting for and reporting of industrial security costs. Eight organizations participated in the field research which was sponsored by the Resources Working Group of the National Industrial Security Program. The research sites span classified and special security programs for the Department of Defense, the Central Intelligence Agency, and the Department of Energy. The objective was to evaluate whether or not cost information could be gathered by a questionnaire on a periodic basis. The research findings include a wide diversity of security cost practices, a lack of uniformity in cost allocations, and differing organization structures for security operations. Several recommendations are made to support an initial cost gathering methodology.

INDUSTRIAL SECURITY COSTS: AN ANALYSIS OF REPORTING PRACTICES

Introduction

There are thousands of private sector organizations, divisions of the largest corporations in the U.S., medium size companies, and small, closely held companies, that contract with the federal government to provide goods and services. As part of the contractual arrangement, federal government organizations such as the Department of Defense, the Central Intelligence Agency, and the Department of Energy impose security requirements on these contractors that add to the normal cost of doing business with the federal government. In recent years there has been growing concern about the cost of these security requirements. The major question is: What is the total cost of industrial security? There is very little knowledge or understanding of the identification, accumulation, and reporting of security costs in the private sector. The objectives of this technical report are to explain the nature and importance of industrial security costing procedures and practices, to evaluate cost methods, and to make recommendations concerning the future collection of security costs.

The National Industrial Security Program

In 1989, as a result of growing concern for escalating security requirements and their accompanying cost, a survey of 14 large aerospace companies in the U.S. was undertaken by the Aerospace Industries Association (Mattice, 1989). This survey was used to support an estimate of industrial security costs of $0.8 billion for these companies for 1989 (Secretary of Defense, 1990, p. 21). For all of industry, some observers projected the total industrial security costs as high as $4 billion. There was mounting pressure to review the entire security requirements of the federal agencies, primarily the Department of Defense (DoD), the Central Intelligence Agency (CIA), and the Department of Energy (DoE).

In 1990, President George Bush directed the National Security Council to prepare a comprehensive review of the concept of a National Industrial Security Program (NISP) as an interagency effort to streamline security requirements, policies, and procedures for the purpose of reducing industrial and federal government security costs. In November 1990, a report to

the President on the NISP was presented by the Secretary of Defense and also signed by the Secretary of Energy and the Director of Central Intelligence (Secretary of Defense, 1990). Thus, it was recommended that the NISP be established and implementation of the program elements proceed. In addition to federal government officials, representatives of industry were to be included in the NISP study and policy making.

A NISP steering committee was appointed and subsequently 11 working groups were established to undertake different portions of the NISP elements. Some items that have emerged thus far are the single scope background investigation (SSBI) and a NISP operation manual (NISPOM).

The major industrial security program involved with cleared contractors is the Defense Industrial Security Program (DISP) of the Department of Defense. This is the source for much of the NISP work. In 1990, DISP included 1.3 million of the 1.5 million cleared contractor personnel and 12,500 of more than 15,000 government cleared contractor facilities. Twenty other federal departments and agencies voluntarily use the services and procedures of the DISP.

Need for a Security Cost Baseline

One of the working groups established by the NISP steering committee was the Resources Working Group. This group was initially tasked to develop procedures for measuring security costs to evaluate the impact on resources of proposed changes in security standards and policies. New security policies and procedures are being decided by other working groups. Since the overall objective of the NISP is to satisfy security requirements while using cost efficient and effective methods, a cost baseline was deemed necessary to assess improvement. Executive Order 12829 (January 1993) is not explicit as to the need for a baseline of security costs, but industry and government officials have proceeded on the basis that such cost determination was necessary. Certainly, each NISP change should be considered in view of cost versus benefits. How the cost baseline can be used in this cost-benefit tradeoff for specific NISP changes is not clear.

In June 1991, the Resources Working Group conducted a questionnaire survey of contractors in the Defense Industrial Security Program to gather information on security operations and costs. The data gathered in that survey were difficult to interpret due to the varying definitions, cost practices, and lack of response to some questions. There still is a

need to better understand the cost base for security requirements. For this reason the feasibility of establishing an industry security cost baseline and annual cost gathering must be carefully considered by the Resources Working Group.

Hierarchy of Security Classifications

There are numerous terms and definitions in the industrial security field that are commonly used and provide a basis for classifying security requirements. The following classifications from the General Accounting Office are useful (GAO, 1993, pp.1-2):

> Classified information is placed in one of three levels--top secret, secret, or confidential--depending on its sensitivity. Some particularly sensitive classified information is further segregated and designated as Special Access Program (SAP) or Sensitive Compartmented Information (SCI).
>
> A security clearance at the appropriate level--top secret, secret, or confidential--is needed to obtain access to classified information. Access to a SAP or SCI requires an additional specific determination and authorization. Because of higher adjudication standards for access to some SAPs and SCI, the denial and revocation of such access often occurs without revocation of the individual's security clearance.
>
> A SAP imposes need-to-know or access controls beyond those normally provided for top secret, secret, or confidential information. Such a program may include, but not be limited to, special clearance, adjudication, investigative requirements, material dissemination restrictions, or special lists of individuals to have a need-to-know.

The number of contractor clearances is difficult to establish. According to the GAO, in 1992, DoD granted over 68,000 SCI accesses and at the end of 1992 there were about 214,500 authorized accesses for DoD and contractor personnel and reservists (GAO, 1993, p. 2). Also, while the number of SAP accesses is unknown, the GAO estimates the number between 200,000 and 250,000 at the end of 1992.

According to DISCO data (Goral, 1993), the following industry total clearances were reported:

Type of Clearance	1990	1991	1992
Confidential	36,896	36,268	47,523
Secret	715,732	613,738	677,488
Top Secret	123,320	137,418	120,331
Totals	875,948	787,424	845,342

There were over 1 million total clearances in industry five years ago, so the number has decreased. There was a steady yearly decrease until 1992 when the total spiked up about

8%. Because of declining DoD expenditures this increase from 1991 to 1992 seems out of line.

Existing Gaps in Understanding Security Costs

Security operations consist of personnel, materials, supplies, phones, alarms, computers, safes, specific buildings and facilities, and any other items necessary to comply with the security requirements of federal agencies. Of interest to the NISP is the cost of the security resources over and above the normal security operations that one would find in an organization that does not contract with the federal government. All organizations, including those not contracting with the federal government, provide security for the workplace, personnel, assets, and information. There are controls so that outsiders cannot access buildings and security systems for preventing access to computers and competitive or proprietary information. There are costs associated with normal or routine security requirements. NISP is concerned with the incremental costs of security to meet federal requirements. That is, industrial security costs should be defined as the added costs from contracting with the federal government on classified projects. It is unlikely that a contractor separates security cost on such an incremental basis.

Security operations in most organizations are a cost center such as a department or function. A cost center means that the security organization's costs are budgeted on an annual basis and the manager of the security organization is responsible for controlling security costs within the budget. The security costs are simply part of the routine budget process for the entire company. As such, they are visible security costs consisting primarily of security personnel and personnel related costs. A headcount of the employees engaged in security operations should be fairly easy to obtain. Likewise, it should not be too difficult to gather the wages, salaries, and benefits costs related to the headcount. Other security costs such as materials, supplies and other physical assets and services may not be easily gathered or identified. This will depend on the type of accounting system and the content of the budget system.

It is possible that some security costs are not included in the security organization's budget. Generally, these would be security costs associated with "black" programs or SAP/SCI contracts. The special security requirements may be budgeted for a "program" or may be specifically identified with a contract. Depending on the organizational arrangements,

these special security requirements over and above classified requirements may be known to the company's security manager but he or she may not have access to specific personnel or costs. In this type of situation, only SAP/SCI program/contract managers may be able to identify security personnel and costs. Gathering security cost data in this type of organization may be very difficult and time consuming. Of course, for SAP/SCI contracts that provide a separate line item of the costs of security requirements, the information is visible and can be collected from contracts. This would still involve some effort. The NISP would be very interested in these costs because this is an area where improvements would most likely occur. The security costs of these special programs is relatively higher than regular classified programs.

Another type of security cost that is of importance to the NISP is the cost of contractor operating personnel and physical assets that are incurred by the contractor but that are not included in the security organization's costs, the cost of special security programs, or specific security costs of a contract. This is another type of invisible cost.

For example, the cost of employee time that is incurred to travel to and attend security briefings, to complete security questionnaires, to accompany visitors, and the two-person rule is charged to the contract or overhead as operating expense and not counted as security costs. The computer security requirements that slow down normal user processing speed due to paragraph markings and other special security codings are not counted as security costs. "Awaiting clearance" or "holding tank" employee time is another example of security cost that is invisible. For this reason, it is necessary to gather information on the number of clearances processed, the number of briefings, the number of visitors, the number of security inspections, and the number of classified documents produced, destroyed, and in inventory. All of these operating activities lead to security costs, yet it is not clear that the data can be easily gathered.

In summary, the above discussion leads to four types of security cost:

1. Normal, routine commercial security costs that would be incurred by a contractor if there was no federal government business. This is impossible to quantify.

2. Visible security costs usually associated with white programs and budgeted and controlled by the corporate security organization.

3. Potentially invisible security costs related to special or black programs that are under

direct control of program or contract managers.

4. Invisible security costs that are related to security tasks, regulations, etc., that lead to increased non-security employee costs that are not recorded as security costs.

The major portion of all categories of security costs are personnel related. Labor costs generally comprise 70% to 80% of security costs in the white world. The remainder are costs of material, supplies, and depreciation for facilities, alarm systems, safes, micro-computers, and other internal or external-contracted services such as computer systems and guards. In the black world, the labor costs may be lower and the non-labor costs may be higher than in the classified programs.

Selection of Security Organizations

A general appeal for volunteer contractors was mailed to professional security organizations. Contractors were asked to participate in a field project to gather data on security cost accounting practices. Members of the Resources Working Group also contacted corporate security managers to participate. Eight security organizations agreed to participate. The resulting collection of volunteer companies does not represent a random sample, but there is no reason to believe that these companies are not representative of security organizations and practices found across all contractors.

The sample of security organizations were three large divisions of very large corporations, three medium size corporations, and two small companies. In addition, one small company provided information by phone and in a written statement. The eight companies that were visited included one Department of Energy contractor. The other sites were engaged in contracts for DoD and CIA customers.

The security manager at each site was contacted to arrange a visit. The objective for the visit was stated as the need to obtain information on the budgeting and accounting for security costs for all classified contracts for the federal government, including the definition of security costs, the allocation of security costs, and operating activity such as the number of clearances, number of briefings, and the number of classified documents. The security manager was asked to arrange interviews with knowledgeable personnel. No formal questionnaire was used for structuring the interviews, but the 1991 questionnaire was used as an informal guide. Thus, the interviews were open-ended.

Personal visits were made to the participating sites during May and June, 1993.

Meetings were held with the director or head of security for the division or company, financial or budget officers, contracting officers, and operating managers responsible for contracts or programs that had classified security requirements or special security requirements. To prevent indentification of companies and individuals, the names of the organizations participating in the research study are being held confidential.

In the following sections, information obtained from the seven DoD/CIA contractors will be presented. The topics will be, in order, the security organization and reporting structure, cost identification and allocation practices, organization changes, recent or planned changes in accounting methods, and availability of security related operating statistics.

Security Organization and Reporting Structure

Site A: Corporate security manager reports to Senior Vice President and General Counsel who reports to the Chief Executive Officer. In addition to Security Department Office and its budget, the security operation is divided into 6 groups each with its own budget. The groups include administration, plant protection, document control, library, and two groups representing local security operations. The business operations of this company consist of seven divisions. Each receives allocated G&A costs. There are 5,850 employees and 80 security employees. Over 95% of the operations are DoD/CIA related.

Site B: The corporate security manager position was recently created, reporting to the president of this small, privately held company. Business operations are divided into 4 divisions, but one of these is dedicated to one customer that is not federal government related. There are 90 employees and 2 security employees. Approximately 50% of the business is with DoD/CIA customers.

Site C: The corporate security manager reports to the Vice President Human Resources & Administration who then reports to the President. The security organization consists of three divisions:

Physical Security Manager
Personnel Security Manager
Special Access Program Administrators (Secure Communications & Computer Security)

There are three business divisions. Total employees are 1,450, including approximately 42 full-time equivalent security employees. Nearly 90% of business is DoD/CIA. Less than 10% is commercial and there is some non-classified federal work.

Site D: The director of security reports to the Vice President Human Resources who reports to the president. The security organization is as follows:

Special Programs Security (SAP/SAR)
Security Services (alarms, locks, investigations, etc.)
Technical Security (TEMPEST, OPSEC, AIS, SSEM, PPP)
DOD Security (DISP Administration, includes Information Security)
Area 1 Security (SCI Admin., DCS, SCI Comm Center)
An another geographical site across the country

There are five separate facility clearances containing over 100 controlled areas. Employees total 5,300 and there are 107 security employees. All business is DoD/CIA related.

Site E: This corporate organization consists of two separate companies. The larger company comprises 75% of operations. The corporate security manager reports to the Executive Vice President Finance and Administration who reports to the president. The security organization consists three geographic regions (east, central, west) and a separate subunit for a separate company. The corporate functions of finance, contracts, human resources, and facility services also report to the Executive Vice President Finance and Administration and each is divided into regions. In a parallel position to the corporate security manager, a separate special security programs director was recently established to manage security for the "covert" SCI/SAP programs. This individual also reports to the EVP Finance & Administration. The corporate security manager is responsible for the "non-covert" SCI/SAP programs. The company recently reorganized its 6 business divisions. Previously, each business division used to handle SCI/SAP security. The new arrangement is to ensure independence. There are 12 cleared facilities. Over 95% of Site E's business is classified DoD/CIA/NASA work. The remaining 5% is commercial work.

Site F: This division of a large corporation reported $800 million sales in the past year. The division is assigned financial responsibility as a profit center with a strong annual budget and strategic planning process. The division is organized into seven business lines and three major units that are treated as cost centers that are allocated to the business lines.

The director of security reports directly to the division president along with other division functions such as finance, human resources, contracts, legal, and technical. Division operations and related security organizations are located in five separate geographic areas. In 1993, there were 288 security employees, down from a peak of 374 in 1991, but still a 10%

increase over the 1990 level. In 1993, classified business is approximately 70% of the total operations or roughly $550 million in sales.

Site G: This division of a large corporation has undergone significant reductions in recent years. It has no commercial business and defense business has fallen significantly. The division is a profit center. Over the last three years, total employees have fallen roughly 40% to 6,646. There are seven separate product lines within this division. The security tasks are included under a director of security, safety, and health. The division security director reports to the vice president of human resources. The security director is responsible for facilities protection, employee safety, security programs, medical, investigations, and employee development. This is a very broad set of responsibilities. In accordance with this organizational arrangement, there are six departments reporting to the security director:

Program Security Manager
Government Security Manager
Occupational Safety & Health
System Security Manager
Investigations Staff Specialist
Plant Protection Executive Officer

There are no SAP contracts at this division. The total budget for security, safety, and health has decreased approximately 25% over the last three years to $5 million.

Cost Identification and Allocation Practices

Site A: The administrative costs of the corporate security manager and allocated central services costs (human resources, telephone) are treated as "general and administrative" costs and allocated as part of "management" cost to all cost centers. Other security costs within the headquarters geographical area (such as personnel, contract guards, library, etc.) are allocated on the basis of "number of employees" to 40 cost centers as overhead. Defense contracts receive overhead allocations. Outside the headquarters area, each site gets an allocation of G&A which includes some security costs and it receives allocations of shared security overhead items (document control, library) and its direct security costs (guards).

Operations budget is $2.8 million of which $1.5 million is for personnel and $.7 is for contract guards. All acquisitions over $1,500 require capitalization and depreciation, but these are accounted for in other accounts (alarms, magnetic card readers, closed circuit TV). For example, GSA containers are acquired as "furniture" and all depreciation expenses are

gathered at the corporate level and allocated accordingly.

There is a transfer price for all computer software and hardware provided to the security operations by the Computer Services Department. The latter has control of all computer and software costs.

The security manager gets involved in the RFP process on questions of security requirements and estimates costs.

Site B: The costs of the security manager and one staff are counted as general and administrative costs and allocated to all divisions. Other security costs are included in overhead (lab supplies, marketing support, administrative accounting, rent, and utilities). Two different bases are used to allocate overhead to three business divisions: judgment and square footage. Contracts receive overhead plus direct security costs. There is no separate security budget. Of the $8 million total operating costs last year, approximately $900,000 was estimated as security costs. Purchases over $1,000 are capitalized and depreciated. This includes computers, safes, copiers, and shredding machines.

The program manager uses Contract Data Requirements List (CDRL) for each RFP and Work Breakdown Schedule (WBS) for security cost based on judgment. This site has not bid on some contracts because of high security requirements.

Site C: The recent total operating costs are $168 million with $1.4 million security costs. Approximately 87% of security costs are labor and labor related costs. Security costs include charges for use of mainframe computer, line charges for computer network and E-mail. The Computer Services department's cost is allocated to all corporate users. The majority of the Security's computer and PC costs are indirect costs. No overhead for non-computer corporate overhead is allocated to Security Departments.

All corporate G&A/overhead (president, senior vice presidents, and vice presidents) is gathered in one lump sum and allocated to three business divisions on the basis of labor hours. Security organization costs are included with human resources corporate G&A/overhead and allocated. Document control cost is in the Library Department's budget which has two elements: conventional and classified DoD. Library's cost is in corporate G&A/overhead as are Security costs. Property depreciation goes into G&A/overhead as a separate line item. If customer objects, G&A/overhead costs may be lowered on a commercial contract. Capital acquisitions in excess of $5,000 are capitalized and depreciation

are direct charges of contracts if required.

A full-time security administrator is a direct charge to a SAP contract plus other security direct labor costs required by the contract. SAP/SAR contracts are charged directly for costs of safes, alarms, locks, shredders, and other material and services as required. There are 6 DoD/CIA contracts.

Site D has a $4.1 million budget for security while total operating costs are $600 million. There are 5 separate budgets for security. The security organization's costs are of two types: those that are included in the cost of human services as G&A/overhead and those direct charges to black programs. The black programs are in two divisions in which security costs are direct charges. Within each black program the security costs are included in "engineering overhead" and allocated to contracts on the basis of direct labor. All AIS costs are part of the Technical Security department which are counted in human resources cost. It is impossible to get an AIS cost breakdown.

Site E's two corporate security managers' salaries (white and black programs) and that of other corporate officers are home office or G&A expenses that are allocated to the two companies on a "total cost input" basis. These allocated corporate costs are included in the Finance and Administration cost pool of each company. The F&A costs are then allocated to business divisions as either overhead or G&A. Security costs are treated as overhead and allocated to divisions on the basis of "sales less subcontracts." Accounting costs are treated as G&A. Thus each business division receives two allocations from corporate: G&A and overhead. For control purposes the company budgets non-black security costs by region. However, the black program security costs are direct charges to the business divisions. Within a division, the security costs can be direct charges of contracts or allocated as overhead to all contracts. Regional security offices can procure capital equipment and will be charged for depreciation and amortization. For computer hardware and software, the business divisions handle all procurement and receive expenses.

Facilities related costs (guards, mail, alarm systems, certain supplies, etc.) are allocated to using departments on either a headcount (e.g., mail) or square footage (e.g. guards) basis. In the recent year, total operating costs were $120 million. Total security costs were $716,000, but this does not include costs of black programs.

Site F: A major accounting change was made recently. In 1992, approximately 17%

of the business consisted of contracts with non-DoD customers, e.g., NASA. These customers complained that, through the overhead charge, they were paying for SCI and other special security requirements that were excessive for their contracts. Following the accounting change, of the 288 security personnel in 1993, 133 are classified as direct costs to security programs and 155 are treated as indirect costs in the overhead cost pool. The accounting change involved a reclassification of indirect security employees' costs into a cost pool that directly benefits "special" security programs. This cost pool is allocated to the special programs. The direct and indirect costs of security operations are gathered into 8 cost pools. The cost pool related to the security management office is classified as G&A cost and allocated with other division G&A costs. There are 4 cost pools that are related directly to specific programs. The "special" security cost pool was allocated to special contracts on a direct labor basis. An intent was to give special security costs visibility "in order to reduce those costs where appropriate." This consisted of $7.6 million of special security costs that were removed from the single overhead pool. The costs remaining in the general overhead pool consisted of labor, depreciation, amortization, rent, etc. The overhead rate for this pool decreased 5% when the special security costs were removed.

Site G has a very complex security cost reporting system. First, there are specific charges to contracts. Starting in 1990 some customers wanted to know specific security costs of their contracts. Therefore, contract proposals for these contracts contain a statement of work with specific security requirements for people, safes, alarms, etc., so that security costs are budgeted as separate line items. Working with customers to direct charge security costs has helped reduce security costs.

Second, as part of the human resources budget, security costs that are not direct charges to contracts are included in overhead/indirect costs. The overhead/indirect cost portion of the security costs were $540,000 in 1992. For example, a major portion of the program security department is allocated to contracts on the basis of manhours while the remaining costs are included in overhead/indirect costs. However, the program security department is all direct charge to contract. The investigations staff and plant protection departments are both treated as overhead/indirect costs.

Capital investments in buildings, alarms, copiers, safes, etc., are the responsibility of the facilities department. Depreciation is charged by the facilities department to security

programs and contracts directly and other depreciation charges are included in overhead. To trace a depreciation charge, you need to know what assets you are depreciating. Communication center operations are direct charges to contracts.

Organization Changes

Site A is on the market. That is, the parent company is attempting to find a buyer for this defense oriented entity. There is a major effort to increase commercial business.

Site B is attempting to increase business and has grown 10% over past 3 years.

Site C is seeking more commercial applications of its technology.

Site D has established a marketing/business development department to increase commercial business. Over the last 3 years, total employees have decreased 15% while the security organization has decreased 30%.

Site E is consolidating all central services for the two separate companies under common ownership.

Site F has established a separate business development organization with the goal of generating new business for the division. Classified business will shrink 10% or more over the next three years while plans call for doubling the non-classified or commercial business.

Site G is undergoing a major organization change in the form of consolidation of two major divisions. This is not likely to impact the local security organization. Since the local division has lost major defense business in the last three years, the security organization will be subject to close budget review. The division and government have reviewed security requirements and technological implications.

Recent or Planned Changes in Accounting Methods

Site A recently changed its budgeting and accounting system to move more costs from its facilities and maintenance category into general and administrative costs. Over 98% of their business is with DoD, so one way or another the costs are going to be charged to defense contracts. A major purpose for this change was to lower the overhead rate for facilities and maintenance costs that are charged to the contracts. However, a higher general and administrative cost allocation rate results. The budget officer stated that this was initiated by the operations management because of concerns on the part of the DoD customers that the facilities and maintenance rate was too high.

Site B is in the process of changing their accounting system to improve the allocation

of overhead costs using measures of the activities.

Site F recently changed its accounting for overhead for special contracts. This was discussed above in the section on cost identification and allocation practices.

Availability of Security Related Operating Statistics

Site A tracks the number of all clearances, briefings, documents, and visits with an automated system. Little effort would be required to gather the data on the annual numbers of these items. No attempt is made to keep track of the manhours related to these activities.

Site B can manually gather data on the numbers of clearances, briefings, documents, and visits, but it will take time and expenses. No manhour data are kept.

Site C has an automated system for tracking clearances, visits, and classified material control. They do not track "holding tank" data. They will have to manually gather briefings and inspections data.

Site D has automated control of clearances and document control, but only the non-SAP briefings are automated. The SAP briefings data would have to be gathered manually. They automatically track the number of inspections. No attempt is made to estimate manhours involved in clearances, briefings, etc.

Site E has automated system for clearances, visits, briefings, and documents control. No attempt is made to estimate manhours involved in clearances, briefings, etc.

Site F has an automated system for clearances, visits, and briefings but a significant effort will be required to consolidate different systems. No attempt is made to estimate manhours involved in clearances, briefings, etc.

Site G can gather data on clearances, visits, briefings, and documents with some effort. There are several locations that are not automated. No attempt is made to estimate manhours involved in clearances, briefings, etc.

Discussion of the Findings

Invisible Costs. A study of seven different security organizations has uncovered a diverse set of accounting practices for security costs. These practices deserve closer examination. First, we will examine a summary of costing practices for a black program. Exhibit A illustrates the security costs for a black program as explained by the program manager. As indicated there are security costs in seven cost categories (identified with an asterisk) that are not captured by the corporate security manager's reports. The only person

who can identify these hidden security costs is the program manager who is thoroughly familiar with the details of the various SAP/SCI or black programs. Also indicated in Exhibit A by the pound sign are security costs that are direct costs of the black security organization. These may be considered visible because they are personnel and personnel related costs. The corporate security manager may not be able to gather this type of security cost information without the help of the black program manager. The point is that none of this information is readily available for completing a NISP cost reporting requirement.

Exhibit A illustrates the difficulty in identifying security costs for special or black programs where contracts do not contain specific line items for security costs. Each contract may have unique security requirements. While the corporate security manager may be asked to review the contract RFP and proposal for estimating security requirements, he or she will not have familiarity with the actual security costs. For large contractors, responsibility for security costs in special or black contracts is placed in the program manager.

The significance of security costs inherent in special or black programs has been noticed by customers. Three of the security organizations have made recent attempts to assign more accurate security costs to the special security programs that require higher, and more costly, security.

Excluded Security Costs. What is not evident in the above details on the different sites' security cost accounting is the missing data. To illustrate this examine the information in Exhibit B on costs that are not included in security costs at one large security organization. The security manager maintains that a portion of these costs should be allocated to security costs. Some of the cost will eventually be allocated to government contracts through overhead allocation, but the visible security costs will be understated. A NISP reporting system would have to ensure that a complete listing of security costs is available and that proper allocations of those costs are included in security costs.

Complexity of Security Organization. The largest corporations usually have one or more very large divisions engaged in DoD or CIA contracts. It follows that the size of the organization correlates with the number of employees and the number of security personnel and costs. Exhibit C contains an example of a large security organization with numerous departments, geographic locations, and cost centers. What is important here is that not all security costs are necessarily contained in one budget. Product lines may have budget

responsibility for certain security departments or geographic operations. While there may be sophisticated accounting systems at the central security location, other locations may not have the same systems. For a corporation, different divisions may classify security costs differently or allocate security costs using different methods. A NISP cost survey must cover each security location that has classified facilities.

Diversity of Security Cost Practices. A reading of the security cost identification and allocation and reporting practices described above for the seven security organizations leads to a wide variety of methods. A summary of the cost practices for different cost items is presented in Exhibit D. The cost items are not an exhaustive list but only some of the major cost items that were uncovered in the research. For example, physical assets and depreciation are not always included in security costs. The costs are sometimes included in overhead and allocated to all contracts. (Recall the items excluded from security costs in Exhibit B.) When a policy is not disclosed in the cell for a particular contractor site, this means that the cost item is included in security organization costs and allocated or assigned as indicated.

To ensure uniformity in reporting security costs, a NISP cost report would have to specify what costs should be included in security costs. If costs are assigned to contracts and the collection of costs will be by contract, there would have to be explicit security cost definitions for the contract. To avoid double counting of security costs, direct charges must be clearly separated from indirect costs.

What is evident from Exhibit D is that there are numerous alternatives for identifying security costs and allocation policies being used by the seven contractors. Note that each of these contractors must comply with the Cost Accounting Standards (CAS) for federal contractors. Exhibit E contains a brief summary of the CAS hierarchy of cost allocations as they would apply to a large company with division and program subunits. Note that the costs continue to accumulate for a CAS covered contract as the costs are allocated down through the organization. This is illustrated by the middle column. Generally, security costs can enter at each organizational level. The problem is that the security costs may be combined with other costs such as human resources as they are allocated through the organization. If security costs are not all direct charges to a CAS covered contract then indirect cost allocations will contain portions of security costs. This was illustrated in Exhibit A.

Small Companies. As confirmed by two small contractors, it is not likely that separate security cost systems are in place. Except for security charges that are allowable as a direct charge to a contract, security costs are included in general and administrative or overhead accounts and allocated to contracts according to the appropriate base (either direct labor or total cost input base). For example, consider the following overhead/indirect cost items:

Security containers are included with capital equipment
Build-out of facilities are included in leasehold improvements
Guards are charged to labor accounts
Alarms are included in leased and equipment rental
Training and education are included in training and education expense

To gather annual security costs for reporting purposes, these companies would have to analyze each G&A/overhead account to identify security items. This would be very time consuming and costly for a small company.

For direct charges to contracts (especially SAP/SCI contracts) it is likely that the program manager and not the security director would be more familiar with the detailed security charges. Unless there is a separate line item for security charges, the contract officer or program manager would have to gather the security cost data on each contract. For management personnel, this would be very costly. In a small company these individuals are very busy running the day to day operations and securing new business.

Likewise, except for general information such as the total employees, the security personnel numbers, and the number of facilities, it is not likely that small companies will have readily available data on the number of clearances, visits, briefings, or document control. Some of this information is available by contract, but not centrally for the entire company. The data are kept manually and can be gathered at some cost.

Rules of Thumb. On the basis of the information gathered there are several trends or rules of thumb that seem to apply. One is that the total security costs for non-special/black programs varies around 1% of total operating costs for the company or division. Without further verification this generalization is subjective. In addition, for these normal cleared programs, security personnel and personnel related costs range from 70% to 80% of total security costs.

For special security or black programs the total security costs as a percent of total

contract costs range higher, from 6-8% to 14% of total costs. One special program manager estimated that total visible and invisible costs could be as high as 40% of the total costs of special programs. The attention to reducing security costs within these programs is understandable. Also, recall that these programs require more non-labor security requirements so that security personnel and personnel related costs are a smaller fraction of total security costs.

Changing Environment. Since 1989, industrial security costs have declined. Due to lower and lower DoD and other federal spending in the classified world, most contractors have downsized in the last 2-3 years. This also includes shrinking the security workforce. Every company seems to be reorganizing and attempting to increase its commercial business.

Another factor that has helped to reduce security costs is the NISP initiative. While not measurable, managers state that the recent NISP actions on the two-person rule and the Tempest requirements have already lowered security costs.

Customers, government security officials, and the contractors themselves are working to reduce security costs. Costs are of more concern today in the global economy and the competition for business contracts. Because of the interaction of these and other factors, the baseline for security costs is moving down and it will be very difficult to attribute savings to specific NISP changes in policies .

Department of Energy Reporting System

Since 1982, the Department of Energy has evolved a detailed budget and reporting system for security costs, or more properly "safeguards and security" costs. Officials at DoE gather annual data from contractors on budgeted amounts in three major categories: operating expenses, capital expenses, and construction. The items contained in each of these categories are listed in Exhibit F. In addition, there are definitions and subclassifications of each category of operating expenses. Each DoE facility must use this classification system to report their budget detail to DoE. In addition, DoE has developed a set of "decision unit" descriptions (e.g., uranium enrichment, weapons, etc.) that contractors must use to budget each operating expense. This is reported for each contractor facility or site. An example of the Protective Forces operating expense subclassifications and decision units is illustrated as follows:

Monterey Flats Nuclear Production

Protective Forces Operating Expenses	TYPES OF DECISION UNITS Uranium Enrichment	Weapons Activities	Nuclear Material Support	Totals
Salaries, wages & benefits				
Materials and supplies				
Equipment and facilities				
Vehicles				
Helicopters				
Training				
Communications				
Management				
Totals				

The purpose of the safeguards and security reporting system is to prepare DoE's annual budget that must be submitted to the Office of Management and Budget (OMB) for review and subsequent submission to the U.S. Congress for budget authorization. Unlike the Defense Department, OMB is actively involved in the DoE budget process. There is a separate budget line for safeguards and security. Thus, DoE contractors must prepare accurate budgets for DoE if they want to have Congressional approval of their annual funding. The DoD budget process is significantly different. There is no separate security or decision unit breakdown for DoD, and OMB does not play an active role in the budget process. DoD budgets by service and program and contractors do not participate in generating data for the service's budget preparation.

Although not all DoE contractors have implemented accounting systems that meet DoE's reporting system, each contractor must prepare the budget data by using accounts, allocations, and judgment on a consistent basis.

It is difficult to see how the DoE security cost reporting system could be adopted for use by DoD contractors. Major expense categories and their breakdown into subclassifications as illustrated in Exhibit F would need to be adopted by defense contractors. This is not the focus of budget and cost control that DoD contractors must practice. Defense contractors bid on specific contracts that have fairly unique missions. The objectives of the work and the security requirements are likely to vary from contract to contract. While the security organizations of DoD contractors have numerous common categories of expenses, there will be very different cost gathering and allocation methods in use.

In summary, is not feasible to adapt the DoE security cost reporting system to DoD

contractors and this system is not further considered.

Recommendations

Any questionnaire to collect industrial security costs will be received with apprehension and skepticism. This is understandable because it is not a requirement of the contract and imposes on management time and resources. Given the myriad accounting practices and organizational arrangements surrounding security costs, a questionnaire should be as simple as possible with minimum detail. The greater the detail the more effort and explanation will be required in the questionnaire design. Thorough pilot testing with a representative sample of security organizations is essential.

Since there are no common accounting practices for industrial security costs, any attempt to prescribe accounting rules will not be well received. Even the choice of cost allocation bases should not be mandated. Proposals for accounting changes for federal contractors must undergo a cost-benefit assessment and review by the current Cost Accounting Standards Board. (No accounting rule-making organization, in the private or public sector, has succeeded in establishing uniform accounting policies. The exceptions are regulatory agencies such as the Interstate Commerce Commission and insurance company regulators.)

It will be best to avoid asking contractors to estimate manhours per briefing, clearance, inspection, and visit. Additional data could be obtained from a small sample of contractors as to the average manhours per briefing, clearance, etc. This constitutes a "benchmarking" type of effort that is currently popular in Corporate America. This is an easier approach to gathering data on the "invisible" security costs. A cross check of the statistical data can be obtained from the DISP data base and other records.

The impact of document handling on security costs is much more difficult. Here too, a benchmarking study of several efficient contractors may be useful. For example, recent benchmarking studies found that efficient companies experience $2.78 to process a payroll check. The production, storing, protection, transporting, and destruction of documents involves major costs in information-intensive special programs.

Three specific recommendations are:

1. Establish line item control for new and renewed special security or black programs by explicitly proposing and programming security costs in the contract. Security costs

will be direct charges to the contract.

2. For the non-special or white security costs, gather the reported security costs but exclude any costs reported within special security programs and allocated non-security costs.

3. Proceed with a benchmarking study of several security organizations that are known to be efficient in meeting security requirements at lowest cost. Gather data on security cost per employee, cost per security employee, security cost as a percent of total costs, average manhours to process clearance, average manhours to process briefing, average manhours per visit, and other measures of performance. Also, obtain information on "reengineering" of security processes to reduce time and costs.

The first two recommendations require action of the NISP to establish an official industrial security cost reporting requirement. The first recommendation is already being practiced in some special programs, so there is a precedent. Much of this effort is implicit for other special programs where the customer is usually actively involved in determining the security requirements and approving the cost budget.

Enacting the second recommendation is more problematic. The biggest hurdle is justifying the additional contractor costs for meeting the reporting requirement. The benefits to be derived must be clear. In a period of shrinking business, security needs, and cost reduction programs this may be difficult. For this reason, an onerous questionnaire must be avoided. A two-page form would be ideal. Additionally, applying the 80-20 rule, the largest 20% of contractors probably contain 80% of the total security costs. For this reason, it may be appropriate to exclude small companies from this security cost reporting requirement.

The third recommendation attempts to capture information on what are the best security practices and what are representative operating statistics for cost efficient and quality security organizations. The 1991 industrial security cost questionnaire provides a useful start. There are average manhour data for operating activities (clearances, briefings, etc.). Other DISP data may be useful in establishing trends for security activities and their costs. These are the invisible costs that are not reported as security costs. Many companies have been using reengineering techniques to lower costs and increase productivity. The professional security community should be asked to identify reengineering efforts and these should be examined.

The following general categories of security costs would be sufficient for both types of programs:

Personnel and related costs--wages, salaries, benefits (management, program security, document control, AIS/Tempest specialist, guards, couriers, escorts, administrative support, and other employees providing direct security services)

Facility costs--owned/depreciation, lease, rent, amortization (buildings, upgrades, phones, alarms, locks, safes, closed circuit television, external lighting, fences, sound proofing)

AIS costs--(computers, software, Tempest)

(**Special programs**--may have additional requirements)

Security operations--number of security employees, number of clearances, number of briefings, number of visits, number of inspections, number of classified documents.

The advantage of these recommendations is that some attempt will be made to gather security costs rather than doing nothing. Security managers should be encouraged to estimate costs where they are not available through reasonable efforts. Further disaggregation of costs will only lead to more effort and the need to define each cost subclassification.

The major drawback to this approach is that the costs will be based on different accounting methods and comparisons between contractors and national averages will not be valid. However, contractors will use their methods consistently, so the trend of security costs for that particular company will be valid. Interperiod comparisons for a single company will have validity. As an added item to the questionnaire for the second year, the contractor may be asked to report the first year's costs.

REFERENCES

Executive Order 12829, The President, **National Industrial Security Program**, Federal Register, January 8, 1993, pp. 3479-3483.

Goral, John, Defense Manpower Data Center, Monterey, California, 1993.

Mattice, Lynn, **Security Cost Survey**, Aerospace Industries Association, 1989.

NISP Resources Working Group, **National Industrial Security Program Security Costs in Industry Survey for Fiscal Year 1990**, June 1991.

Secretary of Defense, **The National Industrial Security Program: A Report to the President**, Washington, DC, November 1990.

EXHIBIT A

Security Costs Within a Black Program
at a Security Organization

Direct Labor	* #
Overhead:	
Indirect labor	* #
Fringes	* #
Facilities	*
DISC	*
F&A Allocation	
G&A:	
Bid & Proposal/IR&D (labor)	* #
Other G&A	
F&A Allocation	*
Company Allocation	
Corporate Allocation	
MIS Allocation	

* Security costs are incurred in this cost item but not visible in the cost system.

This item also includes personnel and related costs incurred by the black security organization.

NOTE: These costs are unknown to the corporate security manager because he is not responsible for special security programs.

EXHIBIT B

Examples of Costs Not Counted As Security Costs
by One Security Organization

Awaiting Clearance Costs
- Holding tank costs are hot issue
- Majority count as overhead, some cases of direct charge to contract
- More complex security requirements, then higher costs

Communications Center Operations and Maintenance
- Costly at $4 million
- Generally counted as overhead of security organization
- Should be related to special security program

Security Escorts
- Counted as either security organization costs or other overhead
- Perhaps a 50-50 allocation

Alarm and Access Control Installation and Maintenance
- Generally not counted security organization's costs
- Should be in security organization's overhead

Facility Modifications to Meet Security Requirements
- Security organization sets policy and writes requirements
- Should be depreciation cost and counted in security overhead

Security Containers--Purchase and Maintenance
- Only person changing combinations included in security organization
- Cost treated as furniture and counted as overhead

Tempest Costs
- Design and installation costs counted in facility organization
- Less of an issue today

Documentation Reproduction
- Some contracts have special requirements
- Security organizations should control document reproduction and costs
- A significant cost item
- May also involve couriers

Program Libraries
- Large number of contracts, is this cost driver?
- Centralized library for large number of contracts
- Some contracts require direct charge

Personnel Related Security Requirements
- Security briefings
- Document accountability and audits
- Polygraph sessions
- PSQ preparation
- Interviews with government security

EXHIBIT C

An Example of the Corporate Organization and Reporting Structure
and the Divisional Security Organization

CORPORATE
$10 Billion Sales
|
GROUP
$1.8 Billion Sales
|
DIVISION
$800 Million Sales
Division President
|
Division Security Manager
Security Operations (314 employees):

12 Security Departments:
- Facility Security
- Policy & Education Security
- Programs Security
- Personnel Security
- Western Systems Security
- Washington Operations Security
- Electronic Security
- Data Security
- NSA Security
- Special Projects Security
- (Specific) AFB Security
- (Separate site) Security

8 Direct/indirect Cost Centers by Programs:
- 4 have all direct personnel assigned to separate programs
- 2 have all indirect personnel which are allocated as either G&A or overhead to program
- 2 have mix of direct and indirect personnel which are allocated to programs

Note: In 1992, overhead related to special programs was placed in a separate pool for allocation to special programs. This decreased the non-special overhead rate by 5%.

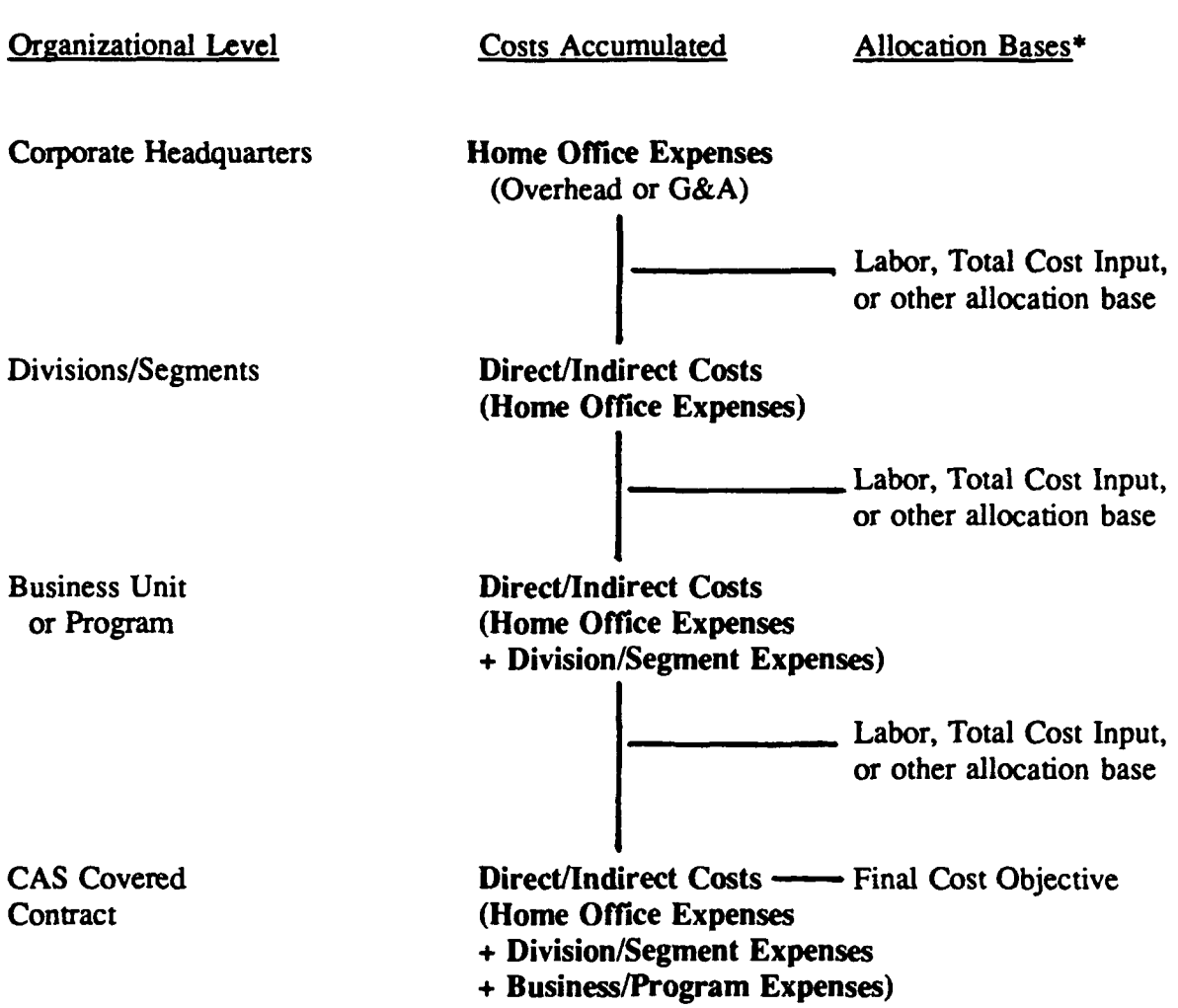
EXHIBIT D
Summary of Costing Practices

COST ITEM	SITE A	SITE B	SITE C	SITE D	SITE E	SITE F	SITE G
Security Director & Staff	G&A	G&A	G&A /labor hours	G&A	G&A; White & Black programs; /total cost input	G&A	G&A
Security Organization Costs (varies)	Overhead /# employees	Overhead /judgment & square footage	G&A, some direct charge to SAP	G&A; Direct Charge to Black Programs, then to Contracts as Engineering Overhead /direct labor	Overhead /sales less subcontracts; Direct charge to Black Programs	Special Programs /direct labor; Other Overhead /direct Labor	Line Item on Special Contracts; Some Overhead /manhours; Other Overhead /other bases
Physical Assets & Depreciation	Other Accounts	Overhead or Direct charges	G&A, Direct charges to SAP	Direct charges	Direct charges to Divisions & Regions, then Overhead /direct labor		Depreciation charge directly to programs & contracts
Facilities: guards, mail, alarm,	Corporate wide allocation				Overhead /headcount or square footage		
GSA containers	Furniture Account, Corporate wide allocation						
Computing/AIS, Hard & software	Transfer price for services		Charged for mainframe, lines, network, E-mail	G&A, no breakdown possible	Direct charge to Division, then overhead		Direct charges
Library	Overhead /# employees		G&A				
Document Control	Overhead /# employees		Part of Library in G&A				
Communication Center							Direct charge to contracts

Note: A slash / precedes the allocation base.

EXHIBIT E

Cost Accounting Standards
Hierarchy of Cost Allocations



* Contractor Disclosure Statement is specific as to direct/indirect cost classifications and use of allocation bases for indirect costs. Each relevant CAS provides general guidelines but federal customer and contractor can agree to other allocation bases under certain conditions.

EXHIBIT F

Department of Energy
Safeguards and Security Functional Categories

Operating Expenses

1. Program Direction
2. Protective Forces
3. Physical Security Protection Systems
4. Transportation
5. Information Security
6. Personnel Security
7. Material Control and Accountability
8. Research and Development

Capital Expenses

1. Program Direction
2. Physical Security
3. Information Security
4. Material Control and Accountability
5. Personnel Security
6. Transportation

Construction

1. General Plant Projects
2. Line Item Construction Projects

Distribution List

Agency	No. of copies
Defense Technical Information Center Cameron Station Alexandria, VA 22314	2
Dudley Knox Library, Code 0142 Naval Postgraduate School Monterey, CA 93943	2
Office of Research Administration Code 08 Naval Postgraduate School Monterey, CA 93943	1
Library, Center for Naval Analyses 4401 Ford Avenue Alexandria, VA 22302-0268	1
Department of Administrative Sciences Library Code AS Naval Postgraduate School Monterey, CA 93943	1
Roger Denk Defense Personnel Security Research 99 Pacific Street Monterey, Ca 93940	4
Department of Administrative Sciences Code AS/Sm Naval Postgraduate School Monterey, CA 94943	4